The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

11/12/2014

SUBJECT:

Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome that could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page containing embedded malicious Adobe Flash code. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There is no known proof-of-concept code available at this time.

SYSTEM AFFECTED:

- Google Chrome Prior to 38.0.2125.122

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium government entities: **High**
- Small government entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple Vulnerabilities have been discovered in Google Chrome, and have been patched in the latest Stable Channel Update. This update addressed multiple bug fixes and security updates including the Adobe Flash vulnerabilities.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Google:

http://googlechromereleases.blogspot.com/2014/11/dev-channel-update_11.html

Adobe:

http://helpx.adobe.com/security/products/flash-player/apsb14-24.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0573

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0574

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0576

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0577

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0581

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0582

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0583

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0584

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0585

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0586

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0588

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0590

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8437

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8438

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8440

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8441

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8442